ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse27952020.pdf

https://doi.org/10.30534/ijatcse/2020/27952020

An effective and robust approach of Image Cryptography using Phase Congruence Correlative method and Arnold Cat Map

Ali Baig Mohammad[1], Tummala Ranga Babu[2]

[1]Research Scholar, ECE Dept., ANU College of Engg. & Tech., Acharya Nagarjuna University, Guntur & Assistant Professor, ECE Dept., Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India, email: mdabaig@gmail.com

[2]Professor & Head, ECE Dept., R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India, email: trbabu@gmail.com

ABSTRACT

In this paper, an effective and robust method of image cryptography scheme is proposed using Phase Congruence Correlative (PCC) method and Arnold Cat Map (ACM). The secret image or a secret watermark is scrambled using ACM method. This scrambled secret image is then embedded into a host image using Adaptive α-β Blending method. The place of embedding in the host image is effectively obtained using PCC method. The embedded image is subjected to various attacks and the secret image is retrieved from the distorted embedded image. This retrieved secret image is compared with the original secret image and various parameters like Peak Signal to Noise Ratio (PSNR), Root Mean Square Error (RMSE), Absolute Difference (AD), Mean Absolute Error (MAE), Maximum Difference (MD) are obtained. This proposed method proves to provide better performance metrics over the past methods.

Key words: Phase Congruence Correlation, Arnold Cat Map, Adaptive α-β Blending, Digital Wavelet Transform, Image cryptography.

1. INTRODUCTION

These days, we are interested in transmitting images over media like internet very often. During this transmission, we must take care of the confidentiality, authenticity, and information content of the images. Sometimes, we may also require transmission of secret information embedded inside images. Several methods like cryptography, steganography, watermarking, etc. are developed for achieving above mentioned factors. During the transmission, the images may be subjected to various types of attacks by the attackers to detect the secret information contained in the images. Robustness to attacks is very important during the transmission of images from the transmitter to the receiver. Despite having several methods for image security provision, the images under transmission are still prone to attacks. The attacker may apply several attacking methods and remain successful in disturbing the information content hidden inside the images to alter the authenticity of the images. So, there is always need for efficient method for ensuring security and preservation of the actual data that is available within the images.

2. RELATED WORK

A typical watermarking algorithm based on Scale Invariant Feature Transform (SIFT), Singular Value Decomposition (SVD) and Discrete Tchebichef Transform (DTT) is proposed in [2]. Rotation, Scale and Translation (RST) attacks are applied on watermarked images and a PSNR of 50dB is obtained. In [2], another colored image watermarking algorithm is proposed. In this paper, Phase congruency method was adopted for the detection of local features of the host image, Arnold Cat Map is used to scramble the watermark and the scrambled watermark is embedded into the blue color band using Adaptive α-β Blending method. Also, the frequency spread in blue color band is less when compared to red and green color bands. The performance parameters obtained in this method are shown in Table 1. The maximum PSNR obtained for a Lena color image using this method proposed in [2] is 54.94dB. Another watermarking algorithm that is robust to RST distortions is proposed in [4]. The watermark is embedded into Fourier Transform of one-dimensional signal. If the image is rotated, the obtained signal is shifted. If it is scaled, the signal is also scaled. And if the image is translated, the signal is unaffected. A maximum PSNR of 38.04dB is obtained in this method. S.N.bal et al in [5] proposed a secured watermarking mechanism based on cryptography and bit pairs matching. They could obtain a maximum PSNR of 52.25dB. C. Y. Lin et al. in [6] proposed an RST resilient watermarking scheme. In [8], Espina et al proposes a new multiple tier information security system using image steganography and authentication using digital signature. They could get a PSNR of 47.72dB.

3. PROPOSED METHOD

The algorithmic steps of the proposed method are depicted in the block diagram illustrated in the Figure 1. The Host image is first read and resized to a size of [256,256]. The R-plane, G-plane and B-plane of the host image are separated out after that. Each colored plane is further divided into spectral bands using Discrete Wavelet Transform with biorthogonal wavelet and a scaling level of 1. Therefore, we obtain four sub-bands of each color plane as [A_R, H_R, V_R, D_R; A_G, H_G, V_G, D_G; A_B, H_B, V_B, D_B]. The Phase Congruency (PC) coefficients for all spectral bands are calculated above are found using the equation (6). The Phase Congruency intercorrelation for all the bands is obtained and the best suited location and optimal band for embedding the secret image are found out by considering the band with highest PC value. The highest PC value indicates the least frequency spread. Now the secret image (to be embedded into the host image) is read and resized to a size of [50,50]. This resized secret image is scrambled using Arnold Cat Map using the equation (7). The scrambling process is carried out column-wise to make the secret image converted into non-distinguishable format. The number of iterations of Arnold Cat Map is used as an encryption key for this method. The same key must be supplied at the decryption side also to retrieve the secret image successfully. This scrambled secret image is embedded into the processed host image using Adaptive α-β Blending method using the equation shown above. In Adaptive α-β Blending method, ‘α’ represents the degree of tolerable distortion of host image and ‘β’ represents the degree of tolerable distortion of secret image after embedding. On the resultant embedded image, Inverse Discrete Wavelet Transform (IDWT) is applied with the embedded band. The resultant image is subjected to various attacks like 'JPG compression', 'Cropping', 'Median', 'Salt & Pepper', 'Rotation'. From the obtained distorted embedded image, the secret image is retrieved using the reverse method indicated by the equation (8). This retrieved secret image is compared with the original secret image and various terms like Peak Signal to Noise Ratio (PSNR), Root Mean Square Error (RMSE), Absolute Difference (AD), Normalized Absolute Error (NAE), Maximum Difference (MD) are obtained. The steps of the algorithm are as shown below:

1) Read the contents of Host image and resize it to [256,256]
2) Extract R,G,B planes of the host image.
3) Apply DWT on three color bands.
4) Compute Phase Congruency (PC) for all spectral bands.
5) Perform PC-intercorrelation for all spectral bands
    a) Compute spectral frequency difference for each plane using the equation shown below:

    $$D_i(p) = PC_i(p) - PC_i(p+1) \qquad (1)$$

    Where, i ϵ A,H,V,D and p ϵ R,G,B
    b) Perform inter correlation for all spectral differences if

    $D_i < D_{i+1}$ → Select Embedding Band as D_1
6) Read the secret image (W) and resize it to [50,50].
7) Scramble using Arnold Cat Map using the equation shown below:

    $$W_k \rightarrow xi_{i+1} = 11\ x_i \bmod N \qquad (2)$$
8) Embed the secret image which is scrambled using Arnold cat Map above into selected band of the host image using Adaptive α-β Blending method shown in the below equation:

    $$B = \alpha B + \beta W_k \qquad (3)$$

9) Perform IDWT with the embedded band (B).
10) Apply attacks.
11) Retrieve secret image using the equations shown below:

    $$W_k = \frac{B - \alpha B}{\beta} \qquad (4)$$

    $$W = \frac{W_k}{11 * ModN} \qquad (5)$$
12) Evaluate performance metrics like PSNR, RMSE, AD, MAE and MD using the equations shown below.

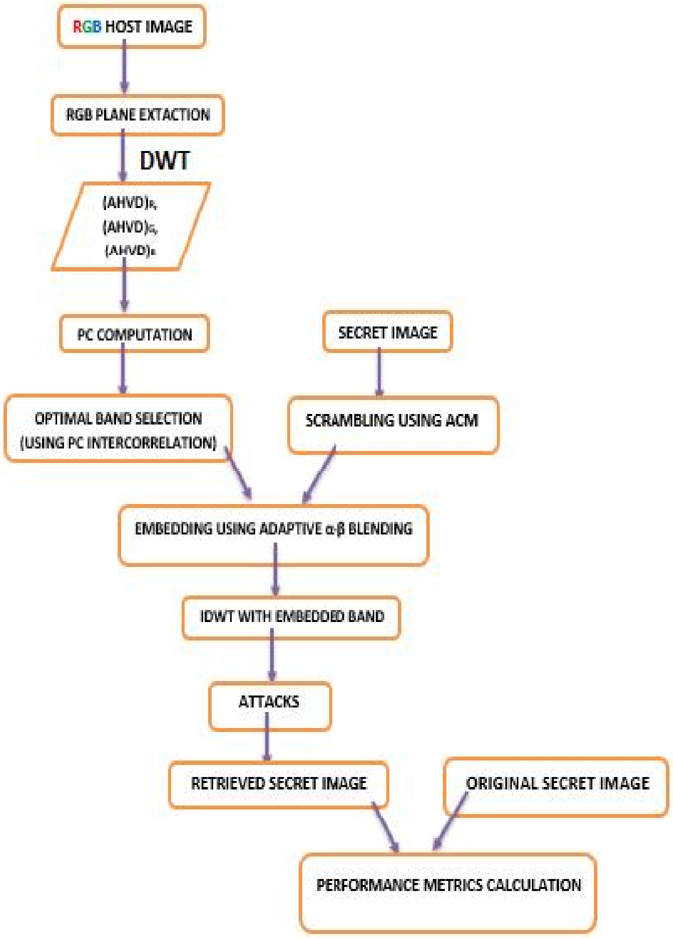


Figure 1: Proposed Block Diagram

4. PERFORMANCE METRICS

4.1 Phase Congruency (PC)

The Phase Congruency (PC) is used for the detection of local features of an image [1]. It specifies the frequency spread in an image. The higher the PC value at a location in an image, the smaller is the frequency spread at that location. After finding all the values of PC of all the color bands, whichever band gives the highest PC is chosen as an optimal band for embedding the secret image into it. In [1], blue color band is chosen as the default band for embedding secret image into it using Adaptive α-β Blending method, whereas in our proposed method, the optimal color band is found based on the highest value of PC. The expression for calculating PC at a particular position in an image is given by the equation (1) below:

$$P(x)=\frac{\sum_{n}V(x)F_n(x)\{\cos(\psi_n(x)-\widehat{\psi}_n(x))-\left|\sin(\psi_n(x)-\widehat{\psi}_n(x))\right|\}-T}{\sum_{n}F_n(x)+\delta} \tag{6}$$

where, $V(x)$ = weights of frequency spread, $F_n(x)$ = filter pair at position x, δ = small positive real number to prevent divide by zero error, T = threshold of the estimated noise influence.

4.2 Arnold Cat Map (ACM)

Arnold Cat Map is used for scrambling the secret image before it is embedded into the optimal color band of the host image. The Arnold Cat Map equation (as given in [1]) is given by the equation given below:

$$\frac{x_{n+1}}{y_{n+1}}=\left[\left(\frac{11}{12}\right)\left(\frac{x_n}{y_n}\right)\right]\bmod N \tag{7}$$

where, (x_n, y_n) and (x_{n+1}, y_{n+1}) are the locations of pixel before and after applying ACM o the secret image and N is the dimension of the secret image. The number of iterations of ACM is used as an encryption key in our proposed method. The same key must be supplied at the time of decryption time also.

4.3 Peak Signal to Noise Ratio (PSNR)

This is the most important performance metric that specifies the degree of reconstruction quality. It is given by the ratio of the maximum possible power of an image to the power of corrupting noise [3]. The higher the value of PSNR, the better is the performance of the algorithm. It is usually expressed in dB. The equation for PSNR in dB is given below:

$$PSNR(dB)=10\log\frac{N^2}{MSE} \tag{8}$$

where N x N is the dimension of the image and MSE is the Mean Squared Error between the original image and the retrieved image.

4.4 Root mean Squared Error (RMSE)

It is a measure of distortion between the retrieved secret image and the original secret image [3]. The smaller the value of RMSE, the better is the performance of the proposed algorithm. The RMSE is calculated using the equation given below:

$$RMSE=\sqrt{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-B_{ij})^2} \tag{9}$$

where N x N is the dimension of the image, A_{ij} & B_{ij} are original secret image and retrieved secret image, respectively.

4.5 Average Difference (AD)

It gives the measure of average of change between the retrieved secret image and the original secret image. The smaller the value of AD, the better is the performance. The value of AD is calculated using the equation given below:

$$AD=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-B_{ij}) \tag{10}$$

4.6 Mean Absolute Error (MAE)

It is an important measure of how much is the retrieved secret image is deviated from the mean value of the original secret image. For better performance, its value must be the least. It can be calculated using the equation given below:

$$MAE=\frac{1}{N}\sum_{i=1}^{N}\left(A_{ij}-\widehat{A}_{ij}\right) \tag{11}$$

4.7 Maximum Difference (MD)

It gives the measure of maximum error between the retrieved secret image and the original secret image. Its value must be as low as possible. The value of MD can be obtained by the equation shown below:

$$MD=Max\left(\left|A_{ij}-B_{ij}\right|\right) \tag{12}$$

5. EXPERIMENTAL OBSERVATIONS

The proposed algorithmic steps are applied on various host images like Lena, Baboon, Peppers, Bird, Flower etc. and secret images using MATLAB 9.8. The experimental observations are as shown below:

Figure 2 shows Lena host image, secret image, Encrypted image, and the retrieved secret image. The performance metrics like PSNR, RMSE, AD, MAE, MD, etc. are calculated using these images and tabulated. Figure 3 shows Baboon host image, secret image, Encrypted image, and the retrieved secret image. Figure 4 shows peppers host image, secret image, Encrypted image, and the retrieved secret image. Figure 5 shows bird host image, secret image, Encrypted image, and the retrieved secret image. The other figures 6, 7 & 8 show the comparison between the conventional method as proposed in [1] and our proposed method based on PSNR, RMSE and AD.

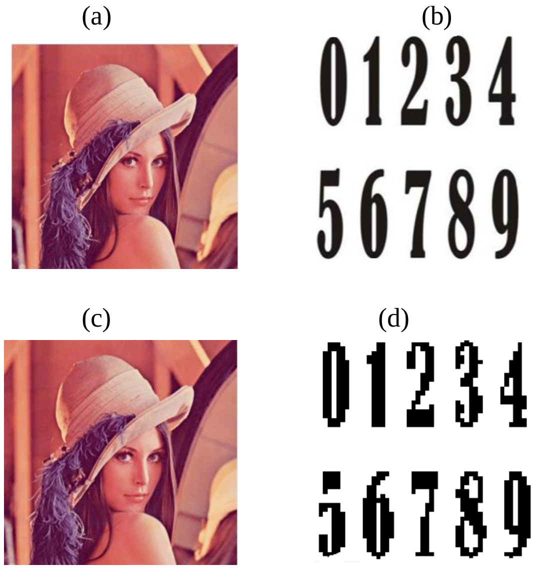


Figure 2: Lena–(a) Host image,(b) Secret Image,(c) Embedded Image,(d) Retrieved secret image

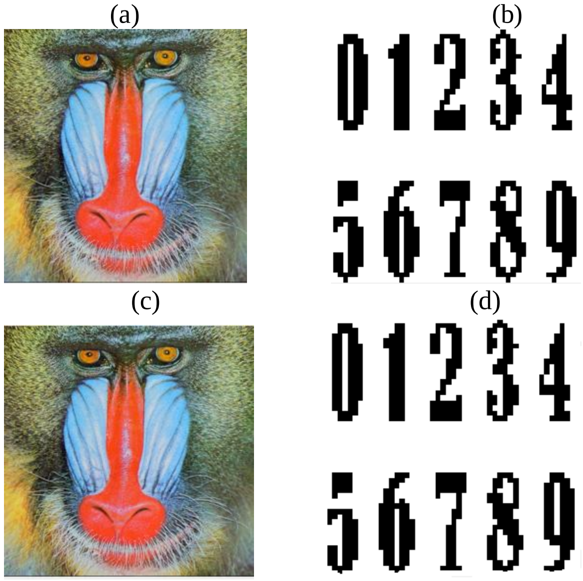
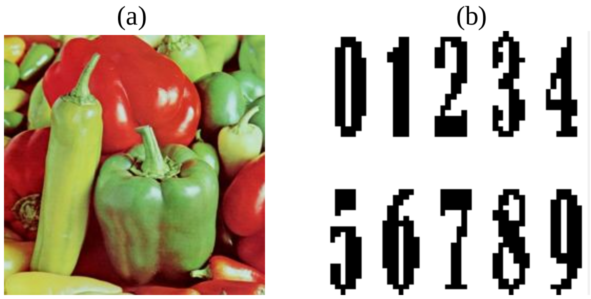


Figure 3: Baboon–(a) Host image,(b) Secret Image,(c) Embedded Image,(d) Retrieved secret image



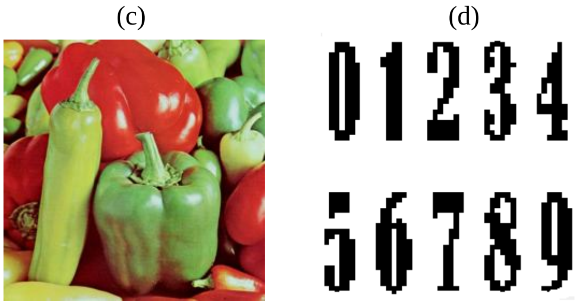


Figure 4: Peppers–(a) Host image,(b) Secret Image,(c) Embedded Image,(d) Retrieved secret image

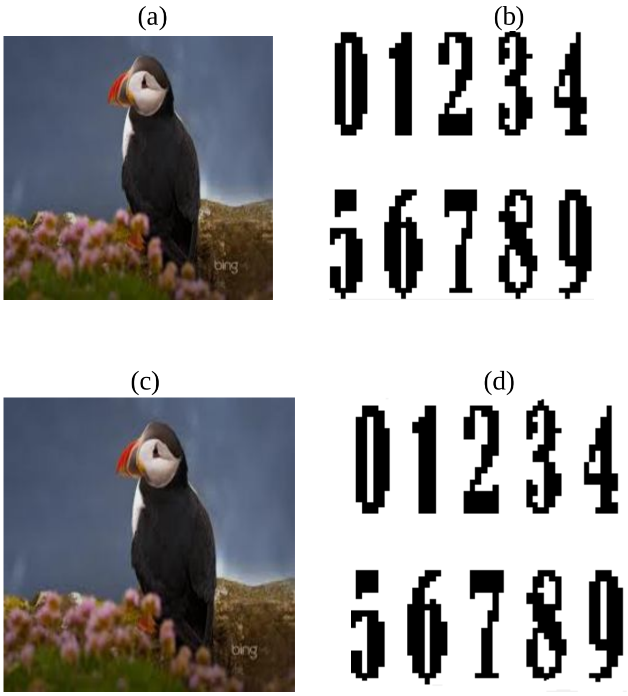


Figure 5: Bird–(a) Host image,(b) Secret Image,(c) Embedded Image,(d) Retrieved secret image

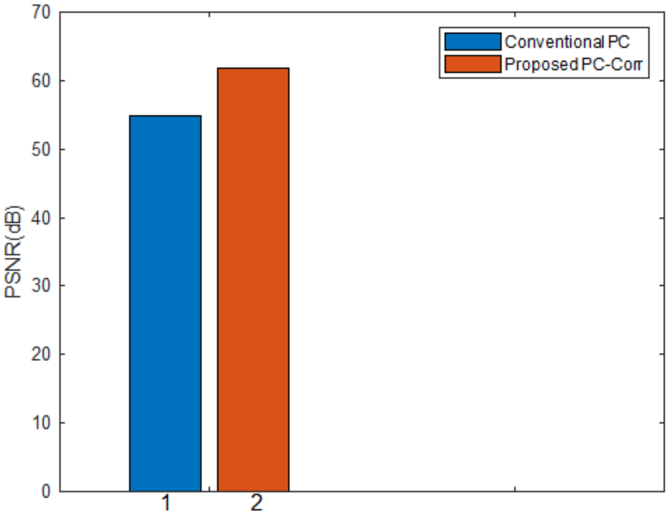


Figure 6: Comparision of PSNR for Lena image

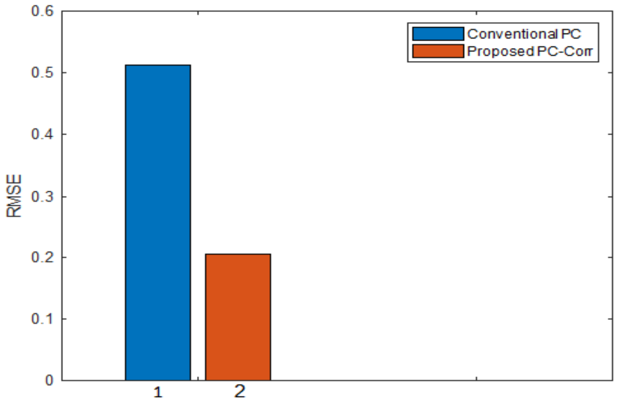


Figure 7: Comparision of RMSE for Lena image

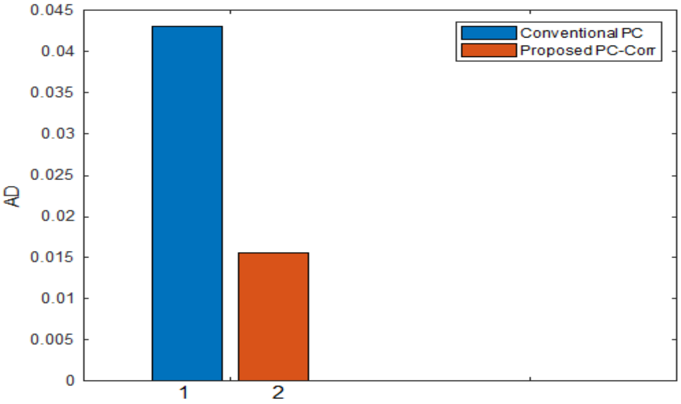


Figure 8: Comparision od Absolute Difference (AD) for Lena image

Table 1: Performance Metrics obtained in [1]

S.No	Performance Parameter	Obtained Value
1	PSNR	54.94dB
2	RMSE	0.5123
3	AD	0.04302
4	MAE	0.0529
5	MD	20.0000

Table 2: Performance Metrics calculated for various host and secret images

Host/Secret	PSNR (dB)	RMSE	AD	MAE	MD
Lena/E3	61.87	0.2056	0.015	0.0139	13.714
Baboon/E3	57.03	0.3507	0.027	0.0243	19.011
Peppers/E3	61.72	0.2092	0.015	0.0142	19.041
Flower/E3	64.72	0.1480	0.011	0.0100	16.630
Bird/E3	67.98	0.1018	0.007	0.0069	11.466

5. CONCLUSION

After implementing the proposed method using MATLAB 9.5, it is observed that the secret image is successfully retrieved from the embedded image. The performance parameters obtained from equations (3) to (7) shown in the Table 2 indicate that the proposed method performs better in hiding the secret image in a set of host images. The PSNR value obtained in this method is as high as 67.98dB. Unlike the proposed method in [1], the band in which the secret image is embedded is dynamically chosen based on Phase Congruency of the bands. This makes the proposed method effective and robust against attacks like compression, rotation, salt and pepper, etc. In [1], the blue color band of the host image is chosen for hiding the secret image into it. Therefore, the phase congruency correlative method helps us in the dynamic selection of the optimal color band for successful concealing of the secret image into it without affecting the host image.

REFERENCES

1. Koley Subhadeep. **A Feature Adaptive Image Watermarking Framework based on Phase Congruency and Symmetric Key Cryptography**. *Journal of King Saud University - Computer and Information Sciences*. Doi: 10.1016/j.jksuci.2019.03.002.
2. Shivani, J, Senapati R.K. (2019). **Feature-Based Robust Image Watermarking Using DTT and SVD for Copyright Protection**. *International journal of simulation: systems, science & technology*. Vol. 9. Doi:10.5013/IJSSST.a.19.06.07.
3. Mustafa, Wan & Yazid, Haniza & Jaafar, Mastura & Zainal, Mustaffa & Abdul Nasir, Aimi Salihah & Mazlan, Noratikah. (2017). **A Review of Image Quality Assessment (IQA): SNR, GCF, AD, NAE, PSNR, ME**. *Journal of Advanced Research in Computing and Applications*. Vol. 7, pp. 1-7.
4. Wang, Xingyuan & Zhu, Xiaoqiang & Zhang, Ying-Qian. (2018). **An image encryption algorithm based on Josephus traversing and mixed chaotic map**. *IEEE Access*. PP. 1-1. 10.1109/ACCESS.2018.2805847. Vol. 6. Pp.23733 - 23746
5. Bal,S.N., et al. **On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching**. *Journal of King Saud University - Computer and Information Sciences*. Doi: 10.1016/j.jksuci.2018.04.0062.
6. C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller. **Rotation, scale, and translation resilient public watermarking for images**, *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.
7. Noor Huda Ja’afar, Syazmeer Sabudin, Afandi Ahmad. **Discrete Curvelet Transform Algorithm for Image Compression System**, International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091, vol. 9, no. 1, pp. 166-169, May 2020.
8. Marilou O. Espina, Arnel C. Fajardo, Bobby D. Gerardo, Ruji P. Medina, **Multiple Level Information Security Using Image Steganography and Authentication**, International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091, vol. 8, no. 6, pp. 3297-3303, November-December 2019.